What is claimed is:

1. A method comprising:

determining whether a key is traceable to one of a set of keys associated with a trusted source;

determining whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of the keys in the set, assigning the key a trusted status.

2. The method of claim 1 further comprising:

verifying the integrity of a document comprising the key and the list of compromised keys.

3. The method of claim 1 wherein determining whether the key is traceable to one of the set of keys further comprises:

reading from a software module embedding the set of keys.

4. The method of claim 1 in which determining whether the key is traceable to one of the set of keys further comprises:

tracing the key through a certificate chain to one of the keys in the set of keys.

5. The method of claim 1 further comprising:

associating a document comprising the key and the set of keys with a software module comprising the set of keys using a hash of the software module in the document.

6. The method of claim 2 in which the document is a manifest signed by the key.

7. The method of claim 1 in which determining whether the key is identified in the list of compromised keys further comprises:

searching the list of compromised keys for the key.

8. A method comprising:

producing a document comprising an identification of a software module and a list of compromised keys; and

digitally signing the document using a key traceable to one of a set of keys comprised by the software module.

9. The method of claim 8 in which the identification of the software module comprises a hash value of the software module.

10. The method of claim 8 in which the key is traceable to one of the set of keys comprised by the software module by way of a certificate chain.

11. The method of claim 8 further comprising:

making the document available on a communication network by which computer systems comprising the software module may read the document.

12. The method of claim 8 in which the set of keys is embedded within the software module.

13. A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause the device to

determine whether a key is traceable to one of a set of keys associated with a trusted source;

determine whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of the keys in the set, assign the key a trusted status.

14. The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

verify the integrity of a document comprising the key and the list of keys.

15. The device of claim 13 further comprising a software module comprising the list of keys.

16. The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

trace the new key through a certificate chain to one of the keys in the set of keys.

17. A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause the device to:

produce a document comprising an identification of a software module and a list of compromised keys; and

digitally sign the document using a key traceable to one of a set of keys comprised by the software module.

18. The device of claim 17 in which the identification of the software module comprises a hash value of the software module.

19. The device of claim 17 in which the key is traceable to one of the set of keys comprised by the software module by way of a certificate chain.

20. An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

determining whether a key is traceable to one of a set of keys associated with a trusted source;

determining whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of the trusted keys,

assigning the key a trusted status.

21. The article of claim 20 in which the instructions, when executed by the processor, further result in:

verifying the integrity of a document comprising the key and the list of keys.

22. The article of claim 20 further comprising a software module embedding the set of keys associated with the trusted source.

23. The device of claim 20 in which the sequence of instructions, when executed by the processor, further result in:

tracing the key through a certificate chain to one of the keys in the set of keys.

24. An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

producing a document comprising an identification of a software module and a list of compromised keys; and

digitally signing the document using a key traceable to one of a set of keys comprised by the software module.

25. The article of claim 24 in which the identification of the software module comprises a hash value of the software module.

26. The article of claim 24 in which the key is traceable by way of a certificate chain to one of the set of keys embedded in the software module.